

УТВЕРЖДЕНО
приказом № 20 от 15.05.2017 г.

**Положение
об обработке и обеспечении безопасности персональных данных,
обрабатываемых в информационных системах персональных данных в
МКДОУ Детский сад 7 с. Красное**

1. Общие положения

1.1. Настоящее Положение об обработке и обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных муниципального казённого дошкольного образовательного учреждения «Детский сад № 7» село. Красное Грачевского муниципального района Ставропольского края (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 № 687.

1.2. Настоящим Положением определяется порядок обработки и обеспечения безопасности персональных данных, при их обработке в информационных системах персональных данных с использованием средств автоматизации и без использования средств автоматизации в муниципальном дошкольном образовательном учреждении детский сад № 4 (далее- ДОУ)

1.3. В настоящем Положении используются следующие понятия:

1.3.1. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

1.3.2. Информационная система персональных данных (далее – Информационная система) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

1.3.3. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других

лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

1.3.4. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.3.5. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

1.3.6. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.3.7. Обработка персональных данных без использования средств автоматизации (далее – Неавтоматизированный способ) – действия с персональными данными, такие как сбор, систематизация, накопление, хранение, использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3.8. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.3.9. Оператор – ДООУ, юридическое или физическое лицо, организующие и осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

1.3.10. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.3.11. Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

1.3.12. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных.

1.3.13. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Порядок обработки персональных данных

2.1. Обработка персональных данных в Информационных системах ДООУ должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2.2. Обработка персональных данных в Информационных системах ДООУ может осуществляться оператором с письменного согласия субъектов персональных данных, за исключением следующих случаев, когда такого согласия не требуется, если:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

2.3. Обработка оператором специальных категорий персональных данных в Информационных системах ДООУ допускается если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;

— персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта

персональных данных невозможно;

обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

2.4. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

2.5. Оператор, получающий доступ к персональным данным, должен обеспечивать конфиденциальность таких данных, за исключением случаев:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

2.6. Обработка персональных данных в Информационных системах ДООУ осуществляется только с согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами, которыми предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2.7. Письменное согласие субъекта персональных данных на обработку своих персональных данных в Информационных системах ДООУ должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

2.8. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных в Информационных системах ДООУ обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

2.9. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в Информационных системах ДООУ дает в письменной форме законный представитель субъекта персональных данных.

2.10. В случае смерти субъекта персональных данных согласие на обработку его персональных данных в Информационных системах ДООУ дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

2.11. Субъект персональных данных имеет право на получение сведений об обработке своих персональных данных в Информационных системах ДООУ, а оператор обязан их предоставить в соответствии со статьями 14 и 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Меры по обеспечению безопасности персональных данных при их обработке

3.1. Безопасность персональных данных, обрабатываемых в Информационных системах ДООУ, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

3.2. Для обеспечения безопасности персональных данных при их обработке в Информационных системах ДООУ осуществляется защита: — информации, обрабатываемой с использованием технических средств; — информации, содержащейся на бумажной, магнитной, магнитно-оптической и иной основе (носителях).

3.3. Работы по обеспечению безопасности персональных данных при их обработке в Информационных системах ДООУ являются неотъемлемой частью работ по созданию Информационных систем.

3.4. Информационные системы ДООУ классифицируются оператором. Проведение классификации Информационных систем определено Порядком проведения классификации информационных систем персональных данных, утвержденным совместным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерством информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20.

3.5. Обмен персональными данными при их обработке в Информационных системах ДОО осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических и программных средств.

3.6. Размещение Информационных систем ДОО, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.7. Безопасность персональных данных при их обработке в Информационных системах ДОО обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее – Уполномоченное лицо). Существенным условием договора является обязанность Уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

3.8. При обработке персональных данных в Информационных системах ДОО безопасность обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременным обнаружением фактов несанкционированного доступа к персональным данным;
- недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянным контролем за обеспечением уровня защищенности персональных данных.

3.9. Защита персональных данных, обрабатываемая в Информационных системах ДОО, обеспечивается за счет средств ДОО в порядке, установленном федеральными законами.

3.10. Доступ сотрудников ДОО к персональным данным, обрабатываемым в Информационных системах ДОО, для выполнения своих должностных обязанностей производится к соответствующим персональным данным на основании списка, утвержденного оператором.

4. Обязанности лиц, имеющих доступ к персональным данным

4.1. Ответственность за обеспечение безопасности персональных данных и надлежащий режим работы Информационных систем ДООУ возлагается на руководителя ДООУ.

4.2. В своей работе сотрудники ДООУ, допущенные к обработке персональных данных в Информационных системах ДООУ, должны руководствоваться требованиями федеральных законов, нормативно-правовых документов Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации, а также настоящим Положением и инструкцией пользователя по защите персональных данных, обрабатываемых в Информационных системах.

4.3. В должностные инструкции сотрудников ДООУ, уполномоченных на обработку персональных данных в Информационных системах ДООУ, должны быть внесены обязанности о необходимости выполнения требований по обеспечению безопасности обрабатываемых ими персональных данных.

4.4. Ответственный за обеспечение безопасности персональных данных в ДООУ руководствуется в своей деятельности инструкцией ответственного за обеспечение безопасности персональных данных, обрабатываемых в Информационных системах ДООУ.

4.5. При обнаружении нарушений порядка предоставления персональных данных, обрабатываемых в Информационных системах ДООУ, оператор незамедлительно приостанавливает предоставление персональных данных пользователям Информационных систем ДООУ до выявления причин нарушений и устранения этих причин.

4.6. За нарушение норм настоящего Положения, а также федеральных законов, регламентирующих порядок обработки и обеспечения безопасности персональных данных, сотрудники ДООУ, допущенные к работе с персональными данными в Информационных системах ДООУ, несут гражданско-правовую, административную, уголовную и дисциплинарную ответственность в соответствии с действующим законодательством.